5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/563,504	06/23/2006	Udo Doebrich	2003P05083WOUS	8240

22116 7590 06/26/2007

SIEMENS CORPORATION
INTELLECTUAL PROPERTY DEPARTMENT
170 WOOD AVENUE SOUTH
ISELIN, NJ 08830

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
06/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/563,504	DOEBRICH ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 January 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/5/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 24-44 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority. ***Information***

Disclosure Statement

3. The information disclosure statement (IDS) submitted on 05 January 2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner has considered the information disclosure statement.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 24-44 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Independent claims 24, 39 and 40 recite in part "applying the first respectively second symmetrical encryption key to data to be transmitted." For purposes of examination, the Examiner shall construe the limitation as "applying the first and second symmetrical encryption keys, respectively, to data to be transmitted." Appropriate correction from the Applicant is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claim 39 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As per claim 39, merely claimed as a computer program representing a computer listing *per se*, that is, descriptions or expressions of such a program and that is, descriptive material *per se*, non-functional descriptive material, and is not statutory because it is not a physical "thing" nor a statutory process, as there are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed aspects of the invention which permit the computer program's functionality to be realized. Since a computer program is merely a set of instructions capable of being executed by a computer, the program itself is not a process, without the computer-readable medium needed to realize the computer program's functionality. In contrast, a claimed computer-readable medium encoded with a computer program defines structural and functional interrelationships between the computer program and the medium which permit the computer program's functionality to be realized, and is thus statutory. **Warmerdam**, 33 F.3d at 1361, 31 USPQ2d at 1760. **In re Sarkar**, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978). See MPEP § 2106(IV)(B)(1)(a).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 24-36 and 39-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,031,913 to Hassan et al., hereinafter Hassan.

10. As per claims 24, 39, and 40, Hassan teaches a method, computer program, and communication system for transmitting data, comprising:

inputting first data originating from a stochastic process into at least first and second users of a communication network (column 3, lines 2-10, column 3, lines 27-44, column 4, lines 3-17, i.e. users A and B measuring impedances of the communication channel);

generating in each of the at least first and second users a symmetrical encryption keys based on the first data (column 3, lines 18-21, column 3, lines 44-59, column 4, lines 50-65, i.e. users generating the same key);

storing the symmetrical encryption key in each of the at least first and second users for transmitting encrypted data between the at least first and second users (column 3, lines 18-21, column 3, lines 44-59, column 4, lines 50-65, i.e. after generating the keys they are stored); and

transmitting the encrypted data between the at least first and second users (column 11, lines 31-46, column 12, lines 17-24), wherein the encrypted data are generated by changing between the encryption keys in a chronological sequence and applying symmetrical encryption keys to data to be transmitted (column 13, lines 45-55, i.e. changing key sequence during a communication session).

11. Hassan does not disclose wherein the first and second users generate first and second keys.

12. It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate first and second keys, since Hassan states at column 13, lines 45-55 that generating two keys so that the key sequence can be changed at predetermined time intervals

during a communication session provides for superior computational and probabilistic secrecy.

13. Regarding claim 25, Hassan teaches wherein generating the symmetrical encryption keys includes generating a plurality of first data by applying a plurality of combinatorial operations to data originating from the stochastic process (column 6, line 48 to column 10, line 47).

14. Regarding claim 26, Hassan teaches wherein the first data are transmitted over the communication network (column 3, lines 2-10, column 3, lines 27-44, column 4, lines 3-17, i.e. users A and B measuring impedances of the communication channel).

15. Regarding claim 27, Hassan teaches wherein the first data are obtained by acquiring at least one measured value from the stochastic process (column 3, lines 2-10, column 3, lines 27-44, column 4, lines 3-17).

16. Regarding claim 28, Hassan teaches wherein the stochastic process includes a time-variable parameter of an automation system (column 3, lines 2-10, column 3, lines 27-44, column 4, lines 3-17, i.e. frequency is a time-variable parameter).

17. Regarding claim 29, Hassan does not teach wherein the first data are obtained from a Least Significant Bit position related to at least one measured value.

18. It would have been obvious to one of ordinary skill in the art at the time the invention was made to obtain the data from a least significant bit position of the measured data, since it is a

well-known and common practice in art to read data from the least significant bit and merely amounts to a design choice.

19. Regarding claim 30, Hassan teaches wherein each of the at least first and second users acquires data originating from the stochastic process for generating the first data (column 3, lines 2-10, column 3, lines 27-44, column 4, lines 3-17).

20. With regards to claim 31, Hassan teaches wherein the first data are generated by applying predefined combinatorial operations to the data originating from the stochastic process (column 6, line 48 to column 10, line 47).

21. With regards to claim 32, Hassan teaches wherein the acquired data originating from the stochastic process are transmitted over the communication network (column 3, lines 2-10, column 3, lines 27-44, column 4, lines 3-17, i.e. communication channel).

22. Regarding claim 33, Hassan does not teach wherein the first and second symmetrical encryption keys are generated upon a request by a master user of the communication network.

23. It would have been obvious to one of ordinary skill in the art at the time the invention was made for one of the users to request the keys be generated, since the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since Hassan does not disclose a third-party for initiating encrypted communications between the two parties.

24. Regarding claim 34, Hassan teaches wherein the first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval (column 13, lines 45-55).

25. With regards to claim 35, Hassan does not teach wherein the first data are transmitted over the communication network at a time of low utilization of the communication network.

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit data over the network at a time of low utilization, since one of ordinary skill in the art would realize that retrieving information about the communication channel when utilization was low would provide for better results without interference from any cross communication occurring on the network.

27. With regards to claim 36, Hassan does not teach wherein the acquired data originating from the stochastic process are transmitted over the communication network at a time of low utilization of the communication network.

28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit data over the network at a time of low utilization, since one of ordinary skill in the art would realize that retrieving information about the communication channel when utilization was low would provide for better results without interference from any cross communication occurring on the network.

29. With regards to claim 37, Hassan does not teach wherein the first data are transmitted using an asymmetrical encryption method.

30. It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the first data with a public key, since one of ordinary skill in the art would recognize that only the recipient's private key would be able to decrypt the data, thereby preventing an unauthorized user from intercepting the data and calculating the symmetric key used to communicate between the two users.

31. With regards to claim 38, Hassan does not teach wherein the acquired data originating from the stochastic process are transmitted using an asymmetrical encryption method.

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the acquired data with a public key, since one of ordinary skill in the art would recognize that only the recipient's private key would be able to decrypt the data, thereby preventing an unauthorized user from intercepting the data and calculating the symmetric key used to communicate between the two users.

33. Regarding claim 41, Hassan teaches wherein the communication network is a public network (column 3, lines 2-10, column 3, lines 27-44, column 4, lines 3-17, i.e. communication channel).

34. Regarding claim 42, Hassan does not teach wherein the communication network is the internet, and the first or second user is a master user for triggering the generating of the first and second symmetrical encryption keys by issuing a request via the internet.

35. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the network to be the internet and for one of the users to request the keys be generated, since the Internet has been well known for more than a decade and the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since Hassan does not disclose a third-party for initiating encrypted communications between the two parties.

36. Regarding claim 43, Hassan does not teach wherein the communication network is an Ethernet.

37. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the disclosed communication channel communicate via the Ethernet protocol, since the Ethernet protocol is well-known and commonly practiced and official notice of such is hereby taken.

38. With regards to claim 44, Hassan does not teach wherein the first or second user is a master user configured to output a command onto the Ethernet for triggering the generation of the first and second symmetrical encryption keys.

39. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the communication channel to be Ethernet and for one of the users to request the

keys be generated, since Ethernet has been well known for more than a decade and the symmetric key generation had to be triggered by one of the two users in order to establish encrypted communications since Hassan does not disclose a third-party for initiating encrypted communications between the two parties.

Conclusion

40. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

41. The following patents are cited to further show the state of the art with respect to calculating a symmetric key, such as:

United States Patent No. 5,745,578 to Hassan et al., which is cited to show a case that is related to the one used to reject the claims of the instant application.

United States Patent Application Publication No. 2006/0190726 A1 to Brique et al., which is cited to show a common technique for formulating symmetric keys.

42. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

43. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

44. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf